UNITED STATES MARINE CORPS
III MARINE EXPEDITIONARY FORCE, FMF
UNIT 35601
FPO AP 96606-5601

ForO P5511.4K
2/SCTYMGR
16 SEP 1992

FORCE ORDER P5511.4K

From: Commanding General
To: Distribution List

Subj: STANDING OPERATING PROCEDURES FOR THE INFORMATION AND PERSONNEL SECURITY PROGRAM (SHORT TITLE: SOP FOR THE INFORMATION AND PERSONNEL SECURITY PROGRAM)

Ref: (a) OPNAVINST 5510.1H
(b) MCO 5510.7F
(c) MCO 5521.3H
(d) FMFPacO P03401.7C (C)
(e) FMFPacO P5510.11F
(f) ForO 2601.2B
(g) NWP (0)
(h) ForO 5210.2F
(i) ForO 5510.16A
(j) ForO 5239.1
(k) CMS 4L
(l) CSP 1A (S)

Encl: (1) LOCATOR SHEET

1. Purpose. To issue command security procedures that specify how the requirements of references (a) through (l) will be accomplished within the III MEF Command Element (CE) and Headquarters and Service Company (HQSVCCo), III MEF.

2. Cancellation. ForO P5511.4J.

3. Background. Reference (a) is the basic controlling regulation for implementation and maintenance of the Department of the Navy's Information and Personnel Security Program. As such it establishes coordinated policies for the security of classified information and for personnel security matters. Reference (b) promulgates instructions concerning personnel security investigations, security clearances and access to classified information for Marine Corps personnel. This SOP supplements references (a) and (b), identifying specific procedures inherent to this command.

4. Action. Heads of General and Special Staff Sections, supervisors and the CO, HQSVCCo will implement the provisions of this SOP and references (a) and (b).

ForO 5511.4K
16 SEP 1992

5. Certification. Reviewed and approved this date.

W. R. MCPHERSON
Chief of Staff

DISTRIBUTION: LIST I

SOP FOR THE INFORMATION AND PERSONNEL SECURITY PROGRAM

RECORD OF CHANGES

Log completed change action as indicated.

Change Number	Date of Change	Date Entered	Signature of Person Incorporated Change

SOP FOR THE INFORMATION AND PERSONNEL SECURITY PROGRAM

CONTENTS

CHAPTER

LOCATOR SHEET

Subj: STANDING OPERATING PROCEDURES FOR THE INFORMATION AND PERSONNEL SECURITY PROGRAM

Location: _____
(Indicate location(s) of copy(ies) of this Manual.)

CHAPTER 1

INTRODUCTION TO THE INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 1

INTRODUCTION TO THE INFORMATION AND PERSONNEL SECURITY PROGRAM

0100. BASIC GUIDANCE. The Information and Personnel Security Program ensures protection of classified information from unauthorized disclosure. This program is divided into four major functional areas: Program Management, Classification Management, Accounting and Control, and Personal Security to facilitate comprehensive implementation. The main stay of this program is ensuring access to classified information is clearly consistent with the interests of National Security.

0101. AUTHORITY. The Commanding General is responsible for establishing and maintaining an Information and Personnel Security Program in compliance with the current editions of OPNAVINST 5510.1, FMFPacO P5510.11 and Foro 2601.2. The command Security Manager is designated as the official primarily responsible for ensuring there is an effective program and that it complies with all the directives issued by higher authority. The Security Manager as the full authority of the Commanding General to issue orders and directives relating to the Information and Personnel Security Program.

0102. APPLICABILITY. This SOP supplements the directives identified in paragraph 0101 above and must be used in conjunction with those directives and others identified herein. Information and personnel security provisions incorporated in other Force Orders and SOPs must comply with the policies and procedures of this SOP and higher headquarters directives.

0103. RESPONSIBILITY FOR COMPLIANCE

1. Heads of General and Special Staff sections, supervisors and the Commanding Officer, HQSVCCo are responsible for implementation and compliance with this SOP.

2. In addition, each individual that deals with classified information is responsible for compliance with this SOP and all identified directives.

0104. SENSITIVE COMPARTMENTED INFORMATION. All Sensitive Compartmented Information (SCI) or Special Intelligence (SI) material received, stored, transmitted and destroyed by III MEF

will be handled and controlled in accordance with established regulations by the Special Security Office (SSO). Access to this information will also be controlled by the SSO.

0105. ATOMIC ENERGY ACT. The Atomic Energy Act of 30 Aug 1954, as amended, and Department of Energy directives regulate the handling, protection and classification of Restricted Data and Formerly Restricted Data. The current edition of OPNAVINST 5510.1 provides for the handling of this information.

0106. WAIVERS. When the requirements of OPNAVINST 5510.1, MCO 5510.7 and this SOP result in untenable sacrifice of operating efficiency, or when there are other sufficient reasons, a waiver of a specific requirement may be requested. Requests for waivers will be submitted to the Security Manager with justification as to why requirements can not be met and describe an alternate procedure. All waivers will be handled on a case by case basis.

0107. ITEMS NOT ADDRESSED. Although this SOP supplements Information and Personnel Security Program directives, it does not address all areas within the program. Policy and guidance in higher headquarters directives are of such length and detail that they have not been incorporated. If guidance on a specific item cannot be found in this SOP, references and identified directives must be consulted. If that fails to answer the question, the Security Manager should be contacted.

CHAPTER 2

PROGRAM MANAGEMENT

CHAPTER 2

PROGRAM MANAGEMENT

0200. BASIC POLICY

1. The Security Manager is the principal advisor on information and personnel security within this CE and is responsible for the management of the program. Any conflicts, recommendations or discrepancies concerning classified information will be forwarded to the Security Manager via the appropriate chain of command.

2. Program control officers, identified in paragraph 0202, are responsible for specific phases of the Information and Personnel Security Program, under the oversight and coordination of the Security Manager.

3. With the exception of SCI/SI information, all classified material received, originated and transmitted by this CE will be processed through the Classified Material Control Center (CMCC) as specified in paragraph 0203.

0201. SECURITY MANAGER

1. The Command Security Manager will be designated in writing (sample format fig. 2-1). The Security Manager must be identified by name to all members of the CE.

2. Prerequisites and duties are specified in the current edition of OPNAVINST 5510.1.

3. Since the Table of Organization for the III MEF CE does not provide for a Security Manager and necessary staff to support the wide range of disparate functions required by the billet, the Security Manager will oversee and coordinate the following functions/cognizant areas:

SECTION	RESPONSIBILITY
G-1/ADJ	Document control (i.e., CMCC functions).
G-2	Advice and assistance on security matters, counterintelligence matters, special access programs and management of Special Security Office functions.
G-3	Operations Security and the World Wide Command and Control System (WWMCCS).

G-4	Security equipment procurement.
G-6	Automated Data Processing (ADP) and communications security.
HQSVCCo	Administrative support (i.e., Manpower Management System queries, request for security clearances, security education, and other administrative duties as stated in this SOP).

0202. PROGRAM CONTROL OFFICERS

1. The below listed control officers will be designated in writing to assist in carrying out an effective security program. Control officers are responsible to the Security Manager and will keep the Security Manager advised on all matters relating to this Order and other referenced regulations. Program Control Officer assignments are singular in nature. No one control officer should be tasked with more than one functional area of responsibility when dealing with the Information and Personal Security Program. All program control officers, assistants and custodians will be appointed in writing using Figure 2-1 as an example format.

a. Top Secret Control Officer (TSCO)

(1) The TSCO is responsible for the receipt, custody, accounting and disposition of all top secret material within this CE in accordance with the specific provisions of OPNAVINST 5510.1, the applicable portions of Force Order 5510.16 and CMS 4L, with the following exception:

(a) SCI material which is controlled by the SSO.

(b) Material contained in special access programs for which the TSCO is not eligible for access. In this case, the Security Manager will determine an appropriate assignment as a control officer for top secret material per the requirements of the special access program and the provisions of the current edition of OPNAVINST 5510.1.

(2) Normally the TSCO billet is filled by the Force Adjutant.

(3) Prereqisites and specific duties are specified in the current edition of OPNAVINST 5510.1.

b. Assistant Top Secret Control Officer (ATSCO). An ATSCO will be appointed to assist the TSCO. The ATSCO will meet the same prerequisites for assignment as the TSCO and will be guided by the same orders as the TSCO. The Secret and Confidential (S/C) Files OIC, under the Force Adjutant, normally is designated as the ATSCO and will be responsible to the TSCO.

c. Top Secret Control Assistant (TSCA). A TSCA may be appointed, when necessary, in accordance with paragraph 2-11.6 of OPNAVINST 5510.1H. TSCAs are directly responsible to the TSCO and will be guided in the performance of their duties by paragraph 2-11.6 of OPNAVINST 5510.1H.

d. OIC, CMCC

(1) The S/C Files OIC is normally assigned as the OIC, CMCC.

(2) The OIC, CMCC, under the staff cognizance of the Force Adjutant, will establish control over and administer accounting procedures for all classified material received, held, originated, transferred or destroyed by this CE. The OIC, CMCC will strictly adhere to the requirements of this SOP, OPNAVINST 5510.1H, MCO 5510.7F and supplemental instructions issued by the Security Manager.

(3) The OIC, CMCC is responsible for publishing detailed internal procedures for the operation of the command's CMCC (CMCC SOP approved by the Security Manager) which will also govern the operation of Secondary Control Points (SCP) and Sub-Custody Control Points (SCCP) pertaining to accountability and control of classified material.

(4) The OIC, CMCC must be a GySgt or above who is a U.S. citizen possessing a final top secret clearance. This individual must demonstrate mature judgment and be completely familiar with the requirements of the duties assigned.

e. NCOIC, CMCC. The NCOIC, CMCC will be appointed, in writing, to assist the OIC, CMCC. The NCOIC, CMCC must be a SNCO and meet the same prerequisites for assignment as the OIC, CMCC.

f. Staff CMS Responsibility Officer. The Staff CMS Responsibility Officer will be a senior officer (O-4 or above), and designated in writing by the Chief of Staff. This officer will assume responsibility for routine CMS matters and sign CMS accounting reports as "Staff CMS Responsibility Officer."

g. Communications Security Material Systems (CMS) Custodian. The CMS Custodian, under the cognizance of the AC/S G-6, is the

responsible officer for all CMS material on charge to the III MEF CMS account. The CMS Custodian will administer the account under the provisions of the current edition of CMS 4L, Communications Security Material Systems Manual, CSP 1A, and other pertinent CMS directives. The CMS Custodian will be assisted in the performance of assigned duties by a CMS Primary Alternate Custodian and two CMS Assistants. Prerequisites for assignment as the CMS Custodian, Alternate Custodian and Assistants as well as the format for Appointment Letters are contained in CMS 4L. The CMS Custodian position will be filled by a GySgt or above.

h. Personnel Reliability Program (PRP) Certifying Officer. The PRP Certifying Officer, under the cognizance of the AC/S, G-3, is responsible for the screening and certification of personnel into the III MEF PRP. The PRP Certifying Officer will be guided by the current editions of MCO 5510.7, FMFPACO PO3401.7, and other directives as applicable.

i. Naval Warfare Publications (NWP) Custodian. The NWP Custodian, under the cognizance of the AC/S, G-3, is responsible for the administration and security of the NWP Library. The NWP Custodian will be guided by the provisions of NWP (0), Naval Warfare Publications Guide.

j. Alternate Control Officer. At least one alternate for the positions listed in paragraph 0202 will be appointed in writing. The Alternate Control Officer will assume the duties only in the event the Primary Control Officer becomes incapacitated or is otherwise not available. The Alternate Control Officer will be guided by the same directives and prerequisites as the Primary Control Officer.

2. Secondary Control Point Custodian (SCPC). Each SCP will appoint a SCPC in writing. The SCPC will receive, establish control of, and administer accounting procedures set forth in the current edition of OPNAVINST 5510.1, this SOP and the CMCC SOP. The SCPC will be filled by a GySgt or above.

3. Secondary Control Point Assistant (SCPA). The SCPA is an administrative assistant responsible to the SCPC for administration, accounting and control procedures for classified material receipted from the CMCC for the SCP. The SCPA will be a SSgt or above.

4. Sub-Custody Control Point Custodian/Alternate (SCCPC/ASCCPC). The SCCPC is the sub-section responsible SNCO; the alternate must be a NCO and both must be appointed in writing. The SCCPC is responsible to the SCPC for the accounting and control procedures for classified items held by the SCCP that have been receipted

from the SCP. The ASCCPC functions in the same manner as the SCCPC in that person's absence, but responsibility for the sub-section classified holdings lies with the SCCPC.

5. Information Systems Security Officer (ISSO). The ISSO, under the staff cognizance of the III MEF Information Systems Management Office (ISMO), G-6, is responsible to the Security Manager for protection of classified information processed on automated word processing equipment and microcomputers within this CE. The ISSO will publish written guidance for the security of hardware and software as pertains to security of classified data. The ISMO will appoint an ISSO and an alternate in writing and provide a copy of the Appointment Letter to the Security Manager.

6. Special Security Officer (SSO)

a. The AC/S, G-2 is assigned as the SSO by the Table of Organization. The SSO is responsible for the Sensitive Compartmented Information Facility (SCIF) and the security, control, dissemination, utilization and destruction of all SCI and SI material.

b. The SSO runs SCI/SI programs independently of the Security Manager. However, there must be cooperation and coordination between the two. The SSO is responsible for advising the Security Manager of the clearance/access status of personnel associated with SCI/SI material. Also, the SSO will provide a copy of all investigation requests/validations to the Commanding Officer, HQSVCCo, as a tickler for official personnel records.

7. Communications Security (COMSEC) Officer. The COMSEC officer, under the staff cognizance of the Communications-Electronics Officer (CEO), G-6, is responsible for the security of military communications within this CE, a principle means of which is the development of classification guides for all communications plans associated with this CE's operations or exercises. The CEO will appoint a COMSEC officer and an alternate in writting and provide a copy of the appointment letters to the Security Manager.

8. Operations Security (OPSEC) Officer. The OPSEC officer is responsible for ensuring security of military operations within the CE, a principal means of which is assignment of classification guides to all operation/exercise plans, systems, programs, or any project involving classified material. Staff cognizance for OPSEC is provided by the AC/S, G-3 who will assign an individual in writing as the III MEF OPSEC officer.

9. WWMCCS Officer. The WWMCCS officer, under the staff cognizance of the AC/S, G-5, is responsible for the security of all WMMCCS classified communications and associated material. The WWMCCS officer will be guided in the performance of these duties by the WWMCCS SOP, this SOP and other pertinent directives.

0203. CLASSIFIED MATERIAL CONTROL CENTERS

1. Classified Material Control Center (CMCC)

a. The CMCC, under the staff cognizance of the Adjutant, houses the command's classified files and records.

b. The CMCC is the central repository for all classified material received, originated or transmitted by this command.

c. The CMCC establishes and maintains control and accountability for all classified material (less SCI/SI material and secret/confidential messages) routed within this command.

d. The CMCC will keep on file authorization letters, results of physical security evaluations, and a personnel security clearance roster. Detailed guidance and procedures for accounting and control are contained in the CMCC SOP.

2. Secondary Control Points (SCP). Each General and Special Staff Section and HQSVCCo is eligible to function as a SCP. A SCP must be approved in writing by the Security Manager. This approval will only be granted after a Physical Security Evaluation (PSE) has been conducted by the section requesting a SCP in accordance with the current edition of OPNAVINST 5510.1. SCPs must maintain a turn-over folder containing detailed instructions for the handling of classified material (per the CMCC SOP), a personnel roster indicating clearance and access of personnel within the section, copy of the PSE and the SCP Letter of Authorization from the Security Manager. Each SCP receives and transmits all classified material through the CMCC. Any classified material recieved from the CMCC must be returned to the CMCC when destruction is required. SCPs are not authorized to destroy classified material other than classified messages. SCP sub-sections may designate SCCPS, which in turn receive and transmit all classified material through the SCCP. A SCCP must adhere to the same procedures as a SCP.

0204. EMERGENCY PLAN. The CE Emergency Plan is contained in reference (h). Heads of General and Special Staff sections

will prepare supporting instructions for the destruction of classified information under their control during an emergency. These instructions will be maintained in the Section SCP Turnover Folder/Desk Top Procedures.

0205. TURNOVER FOLDER/DESK TOP PROCEDURES. Heads of General and Special Staff sections which handle classified information will maintain turnover folders/desk top procedures which will include as a minimum (when applicable) the following:

1. Internal security procedures inherent to individual sections, which should cover what is to be done, who is to do it, and who is to supervise. General statements such as "handle per the provisions of the current edition of ForO P5511.4" are not considered adequate for internal security procedures.

2. Security Manager letter authorizing the storage of classified material.

3. Physical Security Evaluation.

4. Access roster for the section identifying who has been granted access to classified information.

5. Instructions for implementing the Command Emergency Plan.

6. Records of security education as identified in Chapter 3 of this SOP.

7. Reports of unannounced security inspections.

8. Results of Information and Personnel Security Program inspections.

9. Security memorandums or messages originated by the Security Manager.

0206. INSPECTIONS. All Program Control Officers will conduct the required inspections for their cognizant areas in compliance with this SOP and the current edition of OPNAVINST 5510.1.

1. The Security Manager will conduct inspections, both announced and unannounced, in accordance with this SOP and other pertinent directives at the descretion of the Security Manager.

2. Heads of General and Special Staff Sections will require daily inspections of their sections to ensure no classified material is left adrift. When sections physically relocate, whether in garrison or a field environment, the area vacated will be thoroughly inspected to ensure no classified material is inappropriately discarded or left adrift.

LETTER HEAD

_____
(date)

From: Commanding General, III Marine Expeditionary Force
To: Grade, Name, SSN/MOS, USMC

Subj: APPOINTMENT OF (SECURITY MANAGER, TOP SECRET CONTROL OFFICER, ETC.)

Ref: (a) OPNAVINST 5510.1H
(b) ForO P5511.4K

1. Per the provisions of references (a) and (b) you are designated as (List appropriate title) for the III MEF Command Element vice (name of out going individual).

2. Upon completion of your familiarization with the referenced material, you are directed to carry out the duties and responsibilities of this assignment until such time that you are relieved.

3. You will indicate by endorsement hereon acceptance of the duties and note any discrepancies noted during your turnover.

4. You are responsible to the Security Manager for the performance of your duties, whom you will keep informed of all matters of significance.

Chief of Staff

Copy to:
Officer being relieved
OIC, CMCC
Security Manager

_____
(date)

From:
To: Security Manager

1. I have familiarized myself with references (a) and (b) and have assumed duty as (list title).

2. (List results of any required inventories as appropriate).

Figure 2-1.--Sample Format for Appointment Letters.

SOP FOR THE INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 3

SECURITY EDUCATION

CHAPTER 3

SECURITY EDUCATION

0300. BASIC POLICY. The purpose of the Security Education Program is to ensure all personnel understand the need to protect classified information and the proper procedures to safeguard it. The goal is to develop fundamental habits of security to the point that proper discretion is automatically exercised in the discharge of duties, thereby making the security of classified information becomes a natural element of every task. All personnel assigned to this CE, regardless of their position, rank, or grade, are required to actively participate in the Security Education Program as described in this SOP.

0301. INDOCTRINATION

1. Security Manager. The Security Manager will provide guidance, direction, and impetus to the command's Security Education Program, ensuring that an appropriate amount of time is dedicated to security education.

2. CO HQSVCCo. As the focal point for personnel training, the CO, HQSVCCo will, in coordination with the Security Manager, implement the Security Education Program as an integral part of the overall command training curriculum. This program will include annual refresher briefings, counterespionage briefings and media items, (e.g., signs, posters, and Plan of the Week reminders), to ensure continued security awareness. In addition, the CO, HQSVCCo will ensure that all newly joined personnel report to the III MEF AC/S, G-2 Staff Counterintelligence Officer (SCIO) for their Orientation/Initial Security Indoctrination Brief, as part of the "check in" process. This will be accomplished by the inclusion of the AC/S, G-2 (SCIO) on the III MEF check-in sheet.

0302. ON-THE-JOB TRAINING. Supervisors are responsible for ensuring subordinates know the required security procedures for the performance of their duties. The primary responsibility for providing security education is vested in the Heads of General and Special Staff Sections. Accordingly, each General and Special Staff Officer will ensure that the following is accomplished.

1. That all assigned personnel actively participate in the Security Education Program.

2. That each newly joined individual is instructed on the specific procedures for the handling and control of classified material within the section.

3. That all individuals are instructed on the security requirements of their jobs.

4. That records of the above training are maintained in sections' SCP turnover folders/desk top procedures for two years.

0303. REFRESHER TRAINING. Annually, all personnel who have access to classified information are required to receive security education refresher training. This requirement will be satisfied by the CO, HQSVCCo in coordination with the Security Manager. To supplement refresher training, the Security Manager will publish periodic security remainders. These reminders are to be read and initialed by each individual who has access to classified information, filed in the section's SCP turnover folder and maintained for two years.

0304. COUNTERESPIONAGE BRIEFING. This briefing will be scheduled by the CO, HQSVCCo in coordination with the Security Manager once each year, due to annual rotation of personnel within this command. This briefing is required for all personnel who have access to classified information within this command.

0305. SPECIAL BRIEFINGS. Certain types of special briefings are required and will be coordinated by the Security Manager. Personnel requiring such briefings are responsible for informing the Security Manager of their specific requirements.

1. Foreign Travel Briefing. Any individual having access to classified information who plans to travel to/through, or travel on a mode of transportation controlled by a criteria country, or attend a meeting where representatives of communist controlled countries are expected to attend, must receive a defensive security brief. The SCIO will provide this briefing and maintain a record. Upon returning, the individual will be debriefed by the SCIO for any incident that may have security implications. The SCIO will determine if further debriefing by the NISRA, Okinawa is required, and if so, the SCI Officer will arrange for further debriefing.

2. Terrorist Threat Briefing. All personnel having access to classified information who plan to travel to/through high

risk/terrorist threat areas must be given a defensive security briefing. The SCIO will maintain a current list of these areas, provide the briefing and maintain a record of the briefing. Upon returning, personnel will be debriefed by the SCIO, who will determine if further debriefing by NISRA, Okinawa is required, and if so, the SCI Officer will arrange for further briefing.

3. Special Access Programs. Responsible officers for special access programs will ensure that briefing and debriefing requirements are met as required by pertinent directives.

4. Sensitive Compartmented Information (SCI). The SSO is responsible for briefing and debriefing those personnel who have access to SCI information.

0306. DEBRIEFINGS. Those personnel who have had access to classified information must be debriefed under the conditions listed below. The requirements and procedures for debriefings are further described in the current editions of OPNAVINST 5510.1 and MCO 5521.3. The AC/S, G-2 (SCIO) will conduct the debriefings.

1. Prior to termination of active military service or civilian employment, or temporary separation for a period of sixty days or more.

2. In the case of personnel who have been granted limited access, at the conclusion of the access period.

3. When an individual's security clearance is denied or revoked for cause.

4. When an individual is the subject of an administrative withdrawal of security clearance.

5. Prior to transfer to another command.

6. When a person is removed from a nuclear weapons critical or controlled billet in accordance with the current edition of FMFPacO P03401.7.

0307. CONTROL POINT OFFICER TRAINING. The OIC, CMCC will train all CMCC, SCP, SCCP custodians and alternates. Additionally, the OIC, CMCC will provide refresher training to all custodial personnel at least once per quarter.

0702. SECURITY CLASSIFICATION PRINCIPLES

1. Classification Criteria. The current edition of OPNAVINST 5510.1 states that unnecessary classification and higher than necessary classification should be avoided. If there is reasonable doubt concerning the need to classify information, it should be safe-guarded as if it where "Tentative Confidential" pending determination by the OCA. If there is reasonable doubt over the level there is reasonable doubt over the level of classification, it shall be safeguarded at the level pending determination by the OCA. This determination will be made within 30 days of proper submission. Upon classification determination proper marking shall be applied as required by the current edition of OPNAVINST 5510.1 which contains security classification principles, criteria, and consideration.

2. A determination to originally classify shall be made by the OCA, only when the information meets one or more of the criteria listed below and only when the disclosure of the information could reasonably be expected to cause a degree of damage to national security.

a. Military plans, weapons or operations.

b. Foreign government information.

c. Intelligence activities, sources or methods.

d. Foreign relations or foreign activities of the U.S.

e. Vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security.

f. Cryptology.

g. Confidential sources.

h. Scientific, technological, or economic matters relating to national security.

i. U.S. Government programs for safeguarding nuclear materials or facilities.

SOP FOR THE INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 8

DECLASSIFICATION, DOWNGRADING AND UPGRADING

CHAPTER 8

DECLASSIFICATION, DOWNGRADING AND UPGRADING

0800. AUTHORITY. The Commanding General and the Chief of Staff are the only individuals authorized to make decisions concerning declassification, downgrading and upgrading information classified per the current edition of OPNAVINST 5510.1. This authority is limited to information which they classified as OCA. Recommendations for downgrading, declassification or upgrading action will be submitted to the Commanding General via the Security Manager and the Chief of Staff.

0801. ADMINISTRATIVE ACTION. The authority to downgrade or declassify is not to be confused with administrative responsibility of a holder of classified information to downgrade or declassify it as directed by classification instructions, the continued protection guidelines or the instructions on the document. The authority is also not to be confused with a derivative classifier's responsibility to carry forward downgrading and declassification markings.

CHAPTER 9

MARKING

FIGURE

CHAPTER 9

MARKING

0900. BASIC POLICY. The purpose of marking classified material is to inform the holder of the classification level, the degree of protection required, and to assist in extracting, paraphrasing, downgrading and declassification actions. Therefore, all classified material will be marked in a manner that leaves no doubt as to the level of classification assigned to the material, which parts contain or reveal classified information, how long the material must remain classified, and any additional measures necessary to protect the material. The current edition of OPNAVINST 5510.1 provides detailed guidance for marking classified material, including exceptions to basic marking requirements.

0901. ADDITIONAL GUIDANCE. Additional guidance may be found in Chapter II, of the current edition SECNAVINST 5216.5, Department of the Navy Correspondence Manual and Volume V, Joint Operations Planning System.

0902. DEFINITION. Classified material is any product embodying classified information.

0903. DRAFTER RESPONSIBILITIES. The drafter of classified material is responsible to ensure that classified markings are accurately carried forward from source document(s) to the newly created material. Attention to this requirement must start with the initial draft.

0904. APPROVING AUTHORITY RESPONSIBILITIES. Heads of General and Special Staff Sections or individuals with "By direction" authority or message release authority and any individual who approves the creation of classified material is personally responsible for ensuring that classification markings are correctly applied and that adequate records to support the classification markings are maintained.

0905. RECORDS REQUIRED. Records will be maintained by each section which originates classified material. The classification record will be a part of or attached to the file copy of the material.

1. Messages. Per the current edition of OPNAVINST 5510.1, a

"Classified by" line is not required on messages. The originator of the message is considered the responsible classifier and must maintain records to identify the source of the classification.

a. Messages classified under OCA will have a justification statement attached to the originating section's file copy.

b. Messages classified under derivative classification authority will have a listing of source documents attached to the originating section's file copy. A sample format is at Figure 9-1.

2. Material other than Messages. All derivatively classified material other than messages require a "Classified by" line. Originally classified documents require only the signature of the OCA.

a. For derivative classification authority, the "classified by" line must either list a specific source or contain the statement "Multiple Sources." A listing of those sources must be attached to the originating section's file copy.

b. For OCA, the classification justification statement must be attached to the originating section's file copy.

0906. MARKING OTHER CLASSIFIED MATERIAL

1. Maps, Charts and Drawings. The overall classification must be marked at the top and bottom of each document. If the markings might be covered by the customary method of folding or rolling maps, charts and drawings, additional markings that are clearly visible when the document is folded or rolled will be added.

2. Photographs, Transparencies and Slides. When practicable, photographic negatives and positives will be marked with the classification and associated markings and kept in containers that have conspicuous markings. All reproductions of a photograph must clearly show classification and associated markings. For transparencies and slides, the classification and associated markings will be clearly shown on the border, holder or frame and, whenever possible, on the image of each transparency or slide. Additional guidance can be found in the current edition of OPNAVINST 5510.1.

3. Working Papers. Working papers will be marked in accordance with the provisions of paragraph 1006, Chapter 10 of this SOP.

MEMORANDUM

From: (Originating section or individual)
To: File

Subj: CLASSIFICATION AUTHORITY

Ref: (a) (Identify material involved)

1. The reference is classified based on the following sources:

   a. OPNAVINST S5513.4, enclosure (11)

   b. OPLAN 5027, Annex B, Appendix 1

   c. FMFPAC OPORD 201, Annex B, Appendix 1

2. A copy of this memorandum is to be attached to the reference.

J. Q. MARINE

Figure 9-1.-- Sample Format for Recording Classification Authority for Derivatively Classified Material.

HEADING

Subj: LIST SUBJECT AS IN ANY CORRESPONDENCE. TRY TO KEEP THE SUBJECT UNCLASSIFIED AND SHOW CLASSIFICATION AT THE END OF THE SUBJECT LINE (U)

Ref: (a) MCO P1234.1_

Encl: (1) Combined User Manual ( )

1. ( ) Show classification at the beginning of each paragraph;

   a. ( ) and each sub-paragraph.

2. ( ) Mark the TOP and BOTTOM of the page with the highest classification of each page.

SIGNATURE

Classified by: (List source of classification)
Declassify on: (List any declassification instructions)

Figure 9-2.--Sample of Page Markings for Classified Material.

CHAPTER 10

ACCOUNTING AND CONTROL

CHAPTER 10

ACCOUNTING AND CONTROL

1000. BASIC POLICY. Classified information must be afforded a level of accounting and control commensurate with its assigned classification as set forth in the current editions of OPNAVINST 5510.1, ForO 5210.2, ForO 5510.16, CMS 4L, and Chapter 10.

1001. TOP SECRET. The command's TSCO is responsible for receiving, maintaining "cradle to grave" accountability registers for holding, distributing and destroying top secret documents. The TSCO may be assisted in these duties by a Top Secret Control Assistant. These duties include;

1. Ensuring all top secret material is maintained in the CMCC, unless otherwise authorized in writing by the Security Manager.

2. Receive all Top Secret material for the CE.

3. Maintain a detailed accountability register.

4. Conduct page checks according to the current edition of OPNAVINST 5510.1.

5. Due to the frequent transfer of personnel within this command, all top secret documents and material charged to the CE will be physically sighted by the TSCO semiannually and a written record will be maintained.

6. Change of custody inventories will be conducted sufficiently far in advance of relief to permit resolution of any conflicts. The TSCO will not transfer until all conflicts are resolved.

7. All top secret material will be accounted for by a continuous chain of receipts.

8. A record of disclosure will be maintained for each top secret document. This record will include document title, date, name, section and unit of personnel afforded access and signature. All entries must be legibly printed in ink.

9. Provide rosters listing top secret control personnel authorized to receipt for top secret messages.

1002. SECRET AND CONFIDENTIAL. The OIC, CMCC is responsible for the receipt, holding, control, routing, destruction and general accountability of all secret and confidential material within this command. The CMCC SOP for handling classified material contains detailed information on internal accounting procedures. These procedures will include, but are not limited to the following:

1. The CMCC will receive and assign a Local Document Control Number (LDC#), commonly referred to as a "buck tag," to all secret material charged to this command. The LDC# will be the primary means by which the CMCC controls and accounts for secret material.

2. The OIC, CMCC will publish administrative procedures for the accounting, control and destruction of confidential material which does not require a LDC#.

3. Only SCPO, SCPA and personnel designated in writing by the Security Manager are authorized to receipt for classified material from the CMCC.

4. Staff Sections may route secret and confidential material to other sections for review/information (normally for 48 hours or less) without receipts. The section routing the material is liable and must ensure that the material is returned for proper disposition.

5. SCPs and SCCPs are not authorized to transfer classified material outside this command or between SCPs/SCCPs. Classified material requiring transfer outside the CE or between SCPs or SCCPs must be returned to the CMCC for transfer.

6. All LDC# and confidential material received will be returned to the CMCC for destruction.

7. SCPs and SCCPs are not authorized to destroy classified material assigned LDC#s. SCPs and SCCPs may destroy secret and confidential message traffic in accordance with Chapter 17 of this SOP.

8. When personnel having SCP/SCCP responsibilities receive PCS orders, inventories must be conducted and discrepancies reconciled prior to any transfer.

1003. RECEIPT OF CLASSIFIED MATERIAL. All classified material received by this command must be delivered immediately to the CMCC for appropriate processing.

1004. ACCOUNTING FOR SECRET AND CONFIDENTIAL MESSAGES. Secret and confidential messages will be accounted for per paragraph 1000 above.

1005. PROCEDURES FOR THE SCREENING OF INCOMING MAIL. The Force Adjutant will establish a screening point for all incoming mail. This screening point will ensure all incoming mail, bulk shipments and material delivered by courier are adequately protected until a determination is made as to whether they contain classified material.

1006. WORKING PAPERS. Working papers are documents, material, or notes accumulated or created while preparing finished material. When working papers contain classified information the following instructions apply:

1. The top and bottom of each page will be marked with the highest classification of any information contained in the entire document along with the words "WORKING PAPERS."

2. Working papers will be protected in accordance with the classification assigned.

3. The date created will be on the front page of the material.

4. The originator's name and section will be on the front page of the material.

5. The papers will be placed in an appropriate security folder or a security cover sheet will be attached.

6. Working papers maintained for over 90 days must be submitted to the CMCC and have a LDC# assigned or be destroyed.

7. Additional guidance on working papers can be found in the current edition of OPNAVINST 5510.1.

1007. SECONDARY CONTROL POINT PROCEDURES. SCPC will develop written procedures for the handling and control of classified material within their section. The procedures will specify exactly how material is to be acquired, routed, stored, safeguarded and transmitted by the section per the CMCC SOP and this SOP. The written procedures will be maintained in the SCPC turnover folder.

1008. OTHER REQUIREMENTS. Additional accounting and control requirements for special categories of classified material are contained in the current edition of OPNAVINST 5510.1.

CHAPTER 11

PRINTING, REPRODUCTION AND PHOTOGRAPHY

CHAPTER 7

CLASSIFICATION GUIDES

0700. BASIC POLICY. Classification guides are prepared by OCAs for each system, plan, program or project involving classified information. Classification guides are promulgated to assist preparers of classified material in the proper implementation of the Classified Management Program. The OPSEC officer is responsible for the assignment of classification guides to OPLANs, OPORDERs, LOIs, SOPs and any other documents that relate to III MEF operations. OPNAVINST 5513 series promulgates classification guides and OPNAVNOTE 5510 series, semiannually provides an Index of Classification Guides. All members of this Command Element will make maximum use of classification guides when originating classified material. All questions concerning classification guides should directed to the Security Manager.

0701. MAJOR SUBJECT CATEGORY GUIDES. Uniformly formatted classification guides are issued in the following subject categories:

a. OPNAVINST 5513.1; Specific Responsibilities for Preparation, Updating, Administrative Use and Detailed Index.

b. OPNAVINST C5513.2; Air Warfare Programs.

c. OPNAVINST S5513.3; Surface Warfare Programs.

d. OPNAVINST S5513.4; General Intelligence, Cover and Deception, and Investigative Programs.

e. OPNAVINST S5513.5; Undersea Warfare Programs.

f. OPNAVINST S5513.6; Communication and Satellite Programs.

g. OPNAVINST C5513.7; Mine Warfare Programs.

h. OPNAVINST S5513.8; Electronic Warfare Programs.

i. OPNAVINST S5513.9; Nuclear Warfare Programs.

j. OPNAVINST C5513.10; Miscellaneous Programs.

k. OPNAVINST 5513.11; Ground Combat Systems.

l. OPNAVINST S5513.12; Intelligence Research Projects.

m. OPNAVINST S5513.13; Non-Acoustic Anti-Submarine Warfare.

CHAPTER 11

PRINTING, REPRODUCTION AND PHOTOGRAPHY

1100. BASIC POLICY. No classified material will be reproduced by any means unless authorized by the appropriate official listed below. Every effort must be made to minimize the reproduction of classified material.

1. Top Secret. Only the Commanding General may authorize the reproduction of top secret material. This authorization must be in writing. Any request for such reproduction will be submitted in writing via the Security Manager. This request must contain detailed description concerning the document, to include justification for reproduction.

2. Secret and Confidential. Reproduction of secret and confidential material, other than messages, must be authorized by the Security Manager or the OIC, CMCC. The reproduction of said material will be accomplished by CMCC personnel. The CMCC will assign a LDC# to the copy/copies and enter them into the system.

3. Messages. The reproduction of secret and confidential messages may be authorized by the Heads of General and Special Staff Sections and the CO, HQSVCCo. A record of all classified messages reproduced will be maintained by the SCPC or SCCPC. This record will reflect the originator of the material, date reproduced, classification date time group, subject, number of copies produced, distribution and disposition of the reproduced messages.

4. All reproduced material must reflect the classification and other special markings which appear on the original document. In addition each copy will be marked "copy ___ of ___."

1101. REPRODUCTION EQUIPMENT. The CMCC will ensure instructions are posted on or near the machines to ensure the requirements of this SOP are met for the reproduction of classified material.

1102. CONTROL OF PHOTOGRAPHY

1. Individuals photographing III MEF facilities and operations must obtain advance written permission from the Security Manager.

2. Heads of III MEF Staff Sections conducting photographs of award presentations or ceremonial events within their office spaces, must verbally notify the Security Manager.

CHAPTER 12

DISSEMINATION OF CLASSIFIED MATERIAL

CHAPTER 12

DISSEMINATION OF CLASSIFIED MATERIAL

1200. BASIC POLICY. Procedures for disseminating classified material originated or received by this command are contained in this SOP and the directives identified below. The current edition of OPNAVINST 5510.1 contains additional policy and guidance.

1201. DIRECTIVES CONTROLLING DISSEMINATION

1. Dissemination of classified messages will be in accordance with the current editions of ForO 5510.16 and CMS 46.

2. Dissemination of classified material will be per this SOP and the CMCC SOP.

1202. TOP SECRET MATERIAL. Top Secret material will not be disseminated outside this CE without the consent of the originator, higher headquarters, the Chief of Staff, or the Commanding General.

1203. SECRET AND CONFIDENTIAL MATERIAL. Secret and confidential material may be disseminated within this CE and to other agencies in accordance with this SOP, the CMCC SOP, and the current edition of OPNAVINST 5510.1, unless specifically prohibited by the originator. All classified material disseminated within this CE, between SCPs/SCCPs, or outside this CE to other agencies, must be processed through the III MEF CMCC.

CHAPTER 13

SAFEGUARDING

CHAPTER 13

SAFEGUARDING

1300. BASIC POLICY. Classified information or material will be used only within office spaces assigned to and under the complete control of the Commanding General. Requests to use or store information in other areas will be submitted, with detailed justification, to the Security Manager.

1301. RESPONSIBILITY FOR SAFEGUARDING. Anyone who has possession of classified material is responsible for safeguarding it at all times and particularly for securing classified material in appropriate security containers whenever it is not in use or under direct supervision by authorized personnel. Classified information will not be removed from designated office spaces or working areas except in performance of official duties and then only under conditions providing the required protection. Under no circumstances will classified material be removed from official working spaces or taken to personal quarters for personal convenience.

1302. CARE DURING WORKING HOURS. During working hours, the following precautions will be taken to prevent access to classified information by unauthorized persons:

1. When classified documents are removed from storage for working purposes, they will be kept under constant surveillance and face down or covered when not in use. Cover sheets (Figure 13-1) or folders corresponding to the classification of the material will be utilized.

2. Classified information will be discussed only when unauthorized persons cannot overhear the discussion. Passageways, ladderwells, parking lots and social gatherings are inappropriate for discussing classified material. Particular care should be taken when there are visitors or workmen in or around the work area.

3. Preliminary drafts, stenographic notes, working papers and similar items containing classified information will be protected either by destroying them by an approved method or by giving them the same classification and safeguarding them in the same manner as the classified material they contain.

4. Typewriter ribbons and computer disks will be safeguarded and given the highest classification for which they were used. Detailed guidance on computer disks and other magnetic media can be found in Chapter 25 of this SOP.

5. When transporting classified material within this CE cover sheets or folders will be used.

6. At the end of each day all classified and unclassified waste should be either destroyed per Chapter 17 of this SOP or properly safeguarded until it is destroyed. No written material in this CE will be discarded in trash cans.

7. Combinations of security containers will be committed to memory. Combinations will only be stored per the provisions of Chapter 14 of this SOP.

8. Telephone Security. When discussing classified information on a telephone, only STU-III phones will be utilized. The STU-III must be cleared for the level of classified information discussed. Individuals must not "talk around" classified information in the unsecured mode.

9. Security of Facsimile (FAX) Machines. The only FAX machine authorized for transmission of classified material is located in the III MEF Command Center. When sending a classified FAX, the appropriate FAX cover sheet, showing the classification of the information to be faxed, must be utilized. All classified FAXs will be performed by Command Center personnel or as directed by the Chief of Staff.

10. Additional guidance can be found in the current edition of OPNAVINST 5510.1.

1303. SECURITY CHECKS

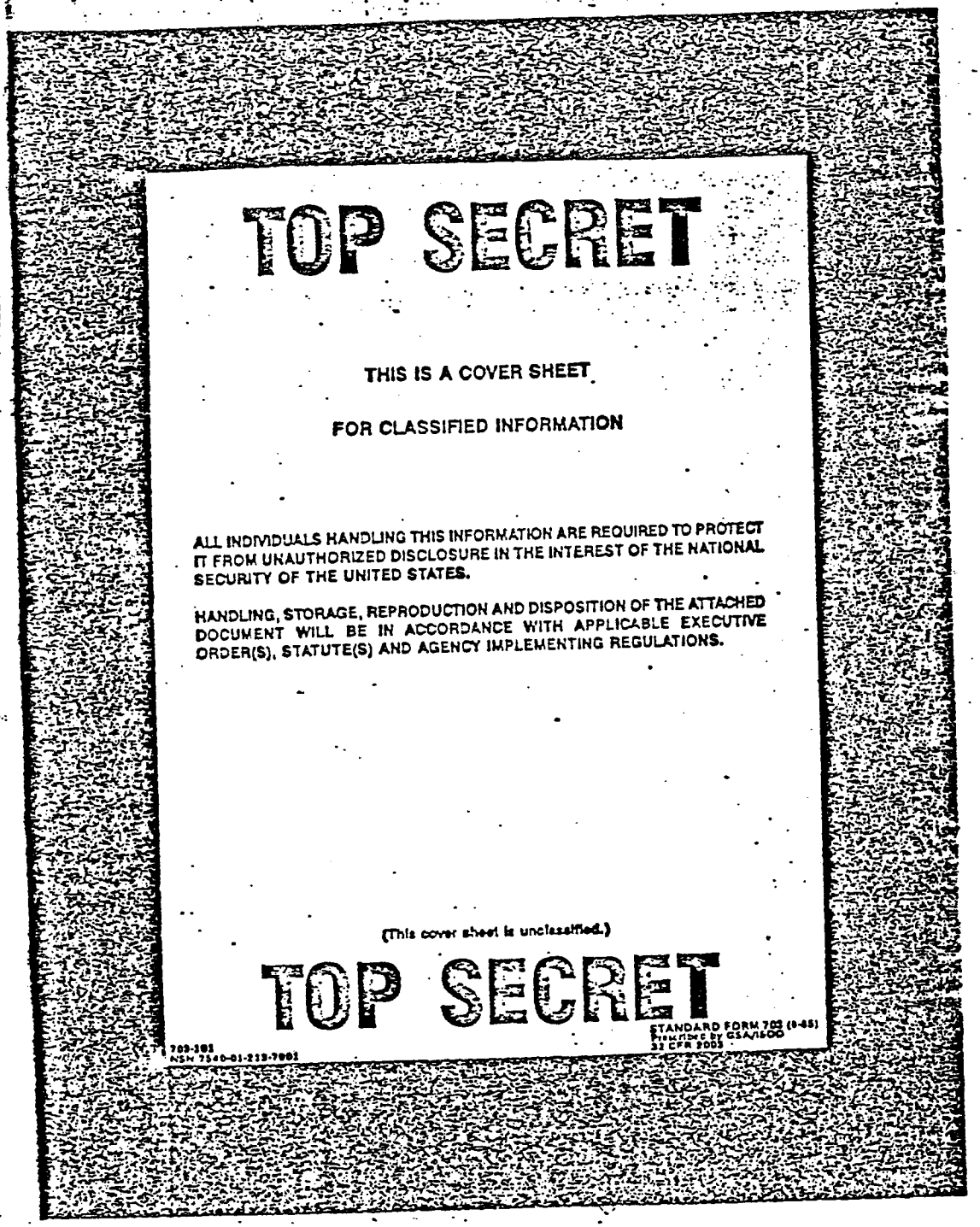
1. Supervisors will require a security check at the end of each working day to ensure all classified material is properly secured. A double check procedure will also be instituted. If there is no one from the section present to perform the double check, Command Center personnel will be utilized. Check sheets (Figures 13-2 and 13-3) will be posted on security containers and near the main entrance to the office spaces to record the results of these inspections.

2. Office spaces within this CE will be subject to inspections both announced and unannounced at the descretion of the Security Manager.

3. When General and Special Staff sections physically relocate office spaces or return from field exercises, the vacated area and all office equipment/furniture will be inspected for classified material left adrift (i.e., behind drawers, cushions, containers, etc.).

4. All burn bags, whether full or empty, will be stored in a security container at the end of normal working hours.

1304. PROHIBITION AGAINST WORKING ALONE. Personnel may not work alone in communication centers, classified libraries, and areas where top secret, SCI or special access program materials are stored. Supervisors will ensure their personnel are familiar with this prohibition and will establish internal procedures to ensure compliance with this requirement.



TOP SECRET

THIS IS A COVER SHEET

FOR CLASSIFIED INFORMATION

ALL INDIVIDUALS HANDLING THIS INFORMATION ARE REQUIRED TO PROTECT IT FROM UNAUTHORIZED DISCLOSURE IN THE INTEREST OF THE NATIONAL SECURITY OF THE UNITED STATES.

HANDLING, STORAGE, REPRODUCTION AND DISPOSITION OF THE ATTACHED DOCUMENT WILL BE IN ACCORDANCE WITH APPLICABLE EXECUTIVE ORDER(S), STATUTE(S) AND AGENCY IMPLEMENTING REGULATIONS.

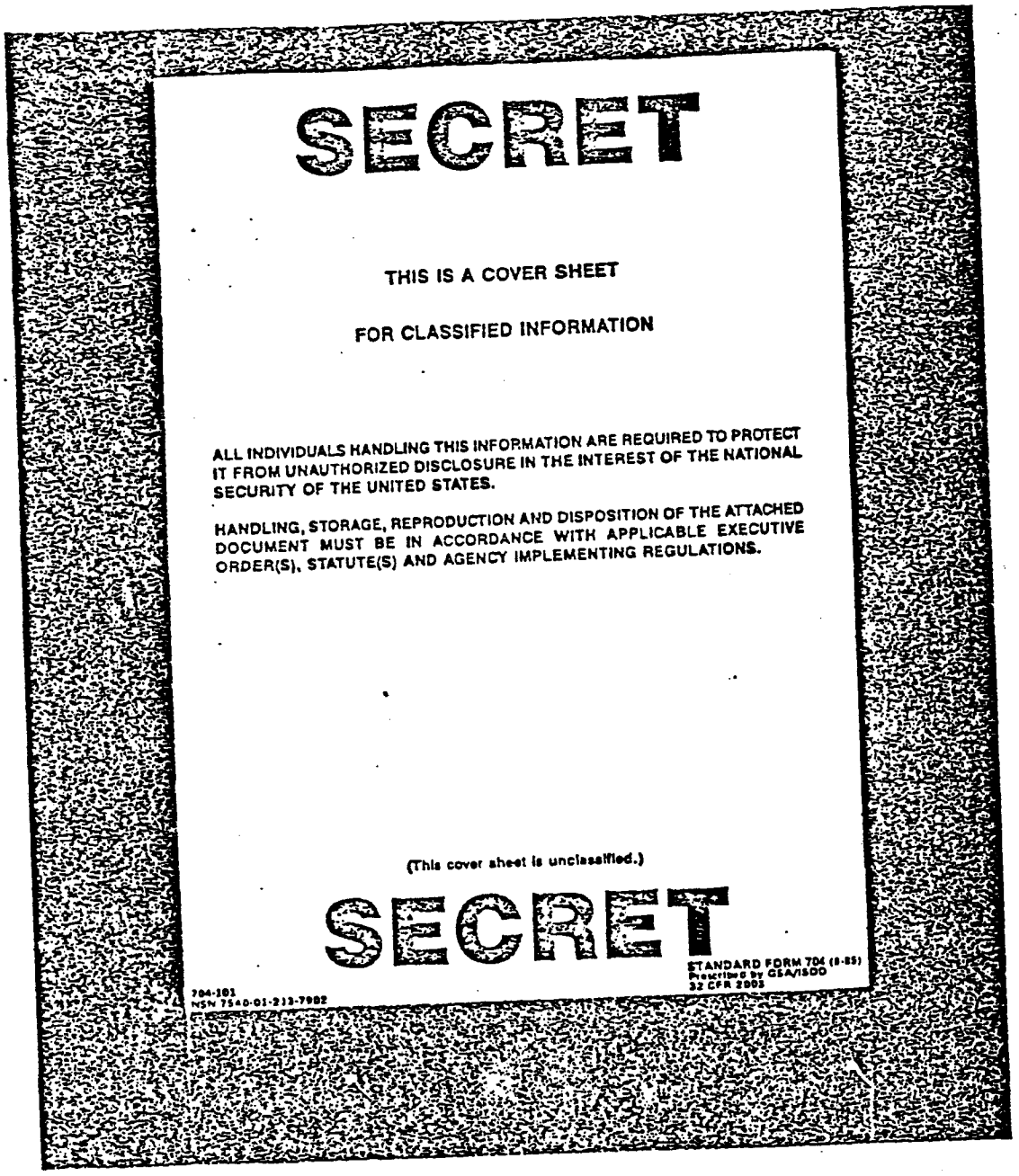
(This cover sheet is unclassified.)

TOP SECRET

703-302
NSN 7540-01-213-7902

STANDARD FORM 703 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

Figure 13-1.--Example of Classified Material Cover Sheet.



SECRET

THIS IS A COVER SHEET

FOR CLASSIFIED INFORMATION

ALL INDIVIDUALS HANDLING THIS INFORMATION ARE REQUIRED TO PROTECT IT FROM UNAUTHORIZED DISCLOSURE IN THE INTEREST OF THE NATIONAL SECURITY OF THE UNITED STATES.

HANDLING, STORAGE, REPRODUCTION AND DISPOSITION OF THE ATTACHED DOCUMENT MUST BE IN ACCORDANCE WITH APPLICABLE EXECUTIVE ORDER(S), STATUTE(S) AND AGENCY IMPLEMENTING REGULATIONS.

(This cover sheet is unclassified.)

SECRET

STANDARD FORM 704 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

704-101
NSN 7540-01-213-7902

Figure 13-1.--Example of Classified Material Cover Sheet--Continued.

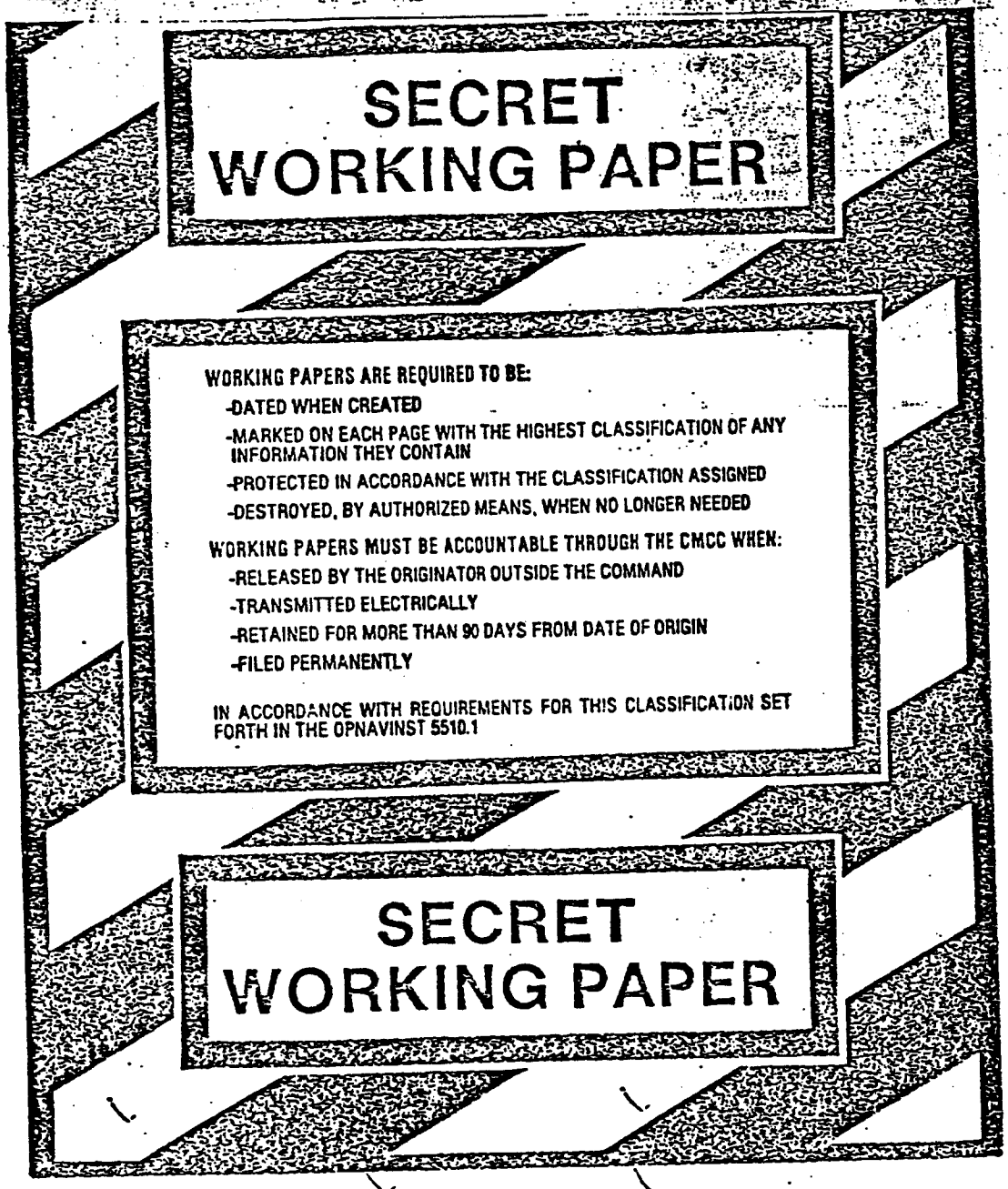
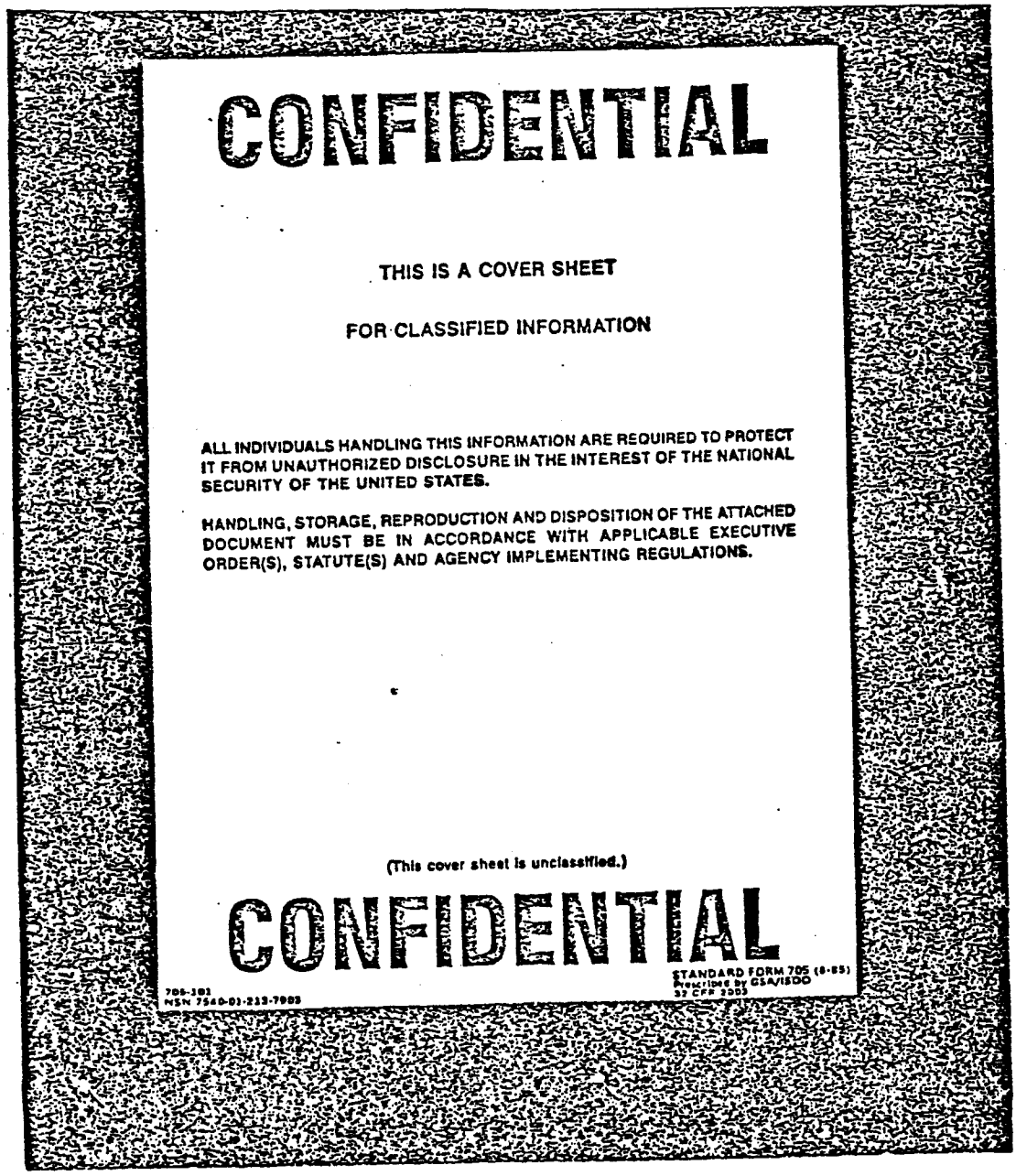


Figure 13-1.--Example of Classified Material Cover Sheet--Continued.



CONFIDENTIAL

THIS IS A COVER SHEET

FOR CLASSIFIED INFORMATION

ALL INDIVIDUALS HANDLING THIS INFORMATION ARE REQUIRED TO PROTECT IT FROM UNAUTHORIZED DISCLOSURE IN THE INTEREST OF THE NATIONAL SECURITY OF THE UNITED STATES.

HANDLING, STORAGE, REPRODUCTION AND DISPOSITION OF THE ATTACHED DOCUMENT MUST BE IN ACCORDANCE WITH APPLICABLE EXECUTIVE ORDER(S), STATUTE(S) AND AGENCY IMPLEMENTING REGULATIONS.

(This cover sheet is unclassified.)

CONFIDENTIAL

705-101
NSN 7540-01-213-7902

STANDARD FORM 705 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

Figure 13-1.--Example of Classified Material Cover Sheet--Continued.

SECURITY CONTAINER CHECK SHEET
(STANDARD FORM 702)

SECURITY CONTAINER CHECK SHEET

TO (If required) | THRU (If required)

CERTIFICATION

I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

MONTH/YEAR

DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (If required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME

FOLD HERE—REVERSE FOLD FOR FULL USE OF BOTH SIDES—FOLD HERE

SECURITY CONTAINER CHECK SHEET

FROM	ROOM NO.	BUILDING	CONTAINER NO.
01 JAN 88	363	WOLF	13

CERTIFICATION

I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

MONTH/YEAR JAN 88

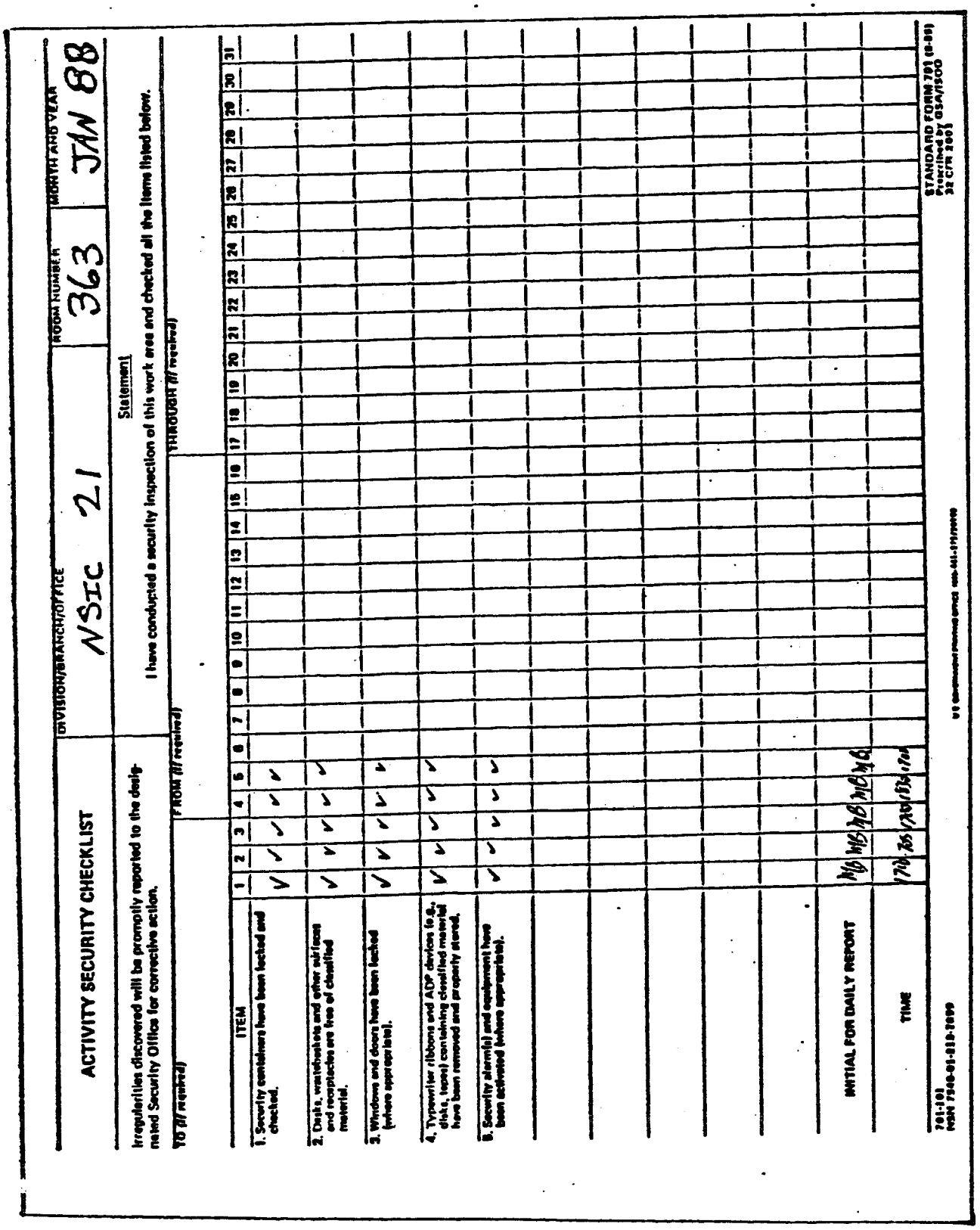
DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (If required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME
1	[illegible]	0800	MB	1700	[illegible]	1700		
2	[illegible]	0700	MB	1705	[illegible]	1705		
3	[illegible]	0700	MB	1700	[illegible]	1700		
4	[illegible]	0650	MB	1530	VP	1530		
5	[illegible]	0650	MB	1700	[illegible]	1700		

STANDARD FORM 702 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

702-101
NSN 7540-01-213-7900

Figure 13-2.--Example of Security Container Check Sheet SF-702.

ACTIVITY SECURITY CHECKLIST
(STANDARD FORM 701)



ACTIVITY SECURITY CHECKLIST

DIVISION/BRANCH/OFFICE: NSIC 21

ROOM NUMBER: 363

MONTH AND YEAR: JAN 88

Statement

I have conducted a security inspection of this work area and checked all the items listed below.

Irregularities discovered will be promptly reported to the designated Security Office for corrective action.

TO (If required) | FROM (If required) | THROUGH (If required)

ITEM	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1. Security containers have been locked and checked.	✓	✓	✓	✓	✓																										
2. Desks, wastebaskets and other surfaces and receptacles are free of classified material.	✓	✓	✓	✓	✓																										
3. Windows and doors have been locked (where appropriate).	✓	✓	✓	✓	✓																										
4. Typewriter ribbons and ADP devices (e.g., disks, tapes) containing classified material have been removed and properly stored.	✓	✓	✓	✓	✓																										
5. Security alarm(s) and equipment have been activated (where appropriate).	✓	✓	✓	✓	✓																										
INITIAL FOR DAILY REPORT				MB	MB	MB	MB	MB																							
TIME				730	735	730	732	730																							

701-101
NSN 7540-01-213-7899

STANDARD FORM 701 (8-85)
Prescribed by GSA/ISOO
32 CFR 2001

Figure 13-3.--Example of Activity Security Checklist SF-701.

CHAPTER 14

STORAGE